インストールガイド - 日本語

ServerView Suite

ServerView Agents V6.12 for Linux

(SUSE, Red Hat, VMware ESX and Citrix XenServer)

2013年2月版

DIN EN ISO 9001:2008 に準拠した 認証を取得

高い品質とお客様の使いやすさが常に確保されるように、

このマニュアルは、DIN EN ISO 9001:2008

基準の要件に準拠した品質管理システムの規定を

満たすように作成されました。

cognitas. Gesellschaft für Technik-Dokumentation mbH

www.cognitas.de

著作権および商標

Copyright © 1998 - 2013 Fujitsu Technology Solutions GmbH.

All rights reserved.

お届けまでの日数は在庫状況によって異なります。技術的修正の権利を有します。

使用されているハードウェア名とソフトウェア名は、各メーカーの商標名および商標です。

Microsoft、Windows、Windows Server、および Hyper V は、米国およびその他の国における

Microsoft Corporation の商標または登録商標です。

Intel および Xeon は、米国 Intel Corporation またはその関連会社の米国およびその他の国にお

ける登録商標または商標です。

目次

目次 3

1 はじめに 5

1.1 アーキテクチャ 7

1.2 本マニュアルの対象者および目的 9

1.3 技術的要件 10

1.3.1 最終段階での変更や修正 10

1.3.2 管理コンソール 10

1.3.3 中央管理用サーバ(CMS) 11

1.3.4 ServerView エージェント 12

1.4 旧版からの変更点 14

1.5 ServerView Suite リンク集 14

1.6 ServerView Suite のマニュアル 16

1.7 表記規則 16

2 管理対象サーバでの構成 19

2.1 BIOS およびファームウェアの設定 20

2.1.1 BIOS の設定 21

2.2 サーバの設定 24

2.3 ServerView のセキュリティコンセプト 26

2.3.1 特定の SET 操作の禁止 26

2.3.2 すべての SET 操作の禁止 26

2.3.3 ユーザ認証による SET 操作 27

2.3.4 SNMP エージェントのオペレーティングシステム固有の特性 29

2.4 SNMPサービスの設定 30

3 ServerView エージェントのインストール 33

3.1 要件 33

3.2 スクリプトベースのインストール 39

3.2.1 ServerView Suite DVD 1 を使用したインストール 40

3.2.2 ディレクトリからのインストール 41

3.3 rpm コマンドを使用するインストール 42

3.4 エラーの考えられる原因 43

3.5 インストール後の ServerView エージェントのメンテナンス 43

3.5.1 srvmagt スクリプト 43

3.5.2 エージェントの設定 46

3.5.3 ServerView エージェントの改善された可用性 48

3.5.4 ServerView エージェントのアンインストール 49

3.5.5 ServerView エージェントの開始と停止 49

3.5.6 補足情報 50

3.5.7 管理ユーザの設定 51

3.5.8 インストール後のコンピュータ情報の変更 52

3.5.9 アップデートインストール/カーネルのアップデート 53

3.5.10 パフォーマンスマネージャによるレポートの出力 54
3.5.11 /tmp ディレクトリ配下の一時ファイル 54
3.5.12 syslog のソース名 55
3.6 APC UPS の設定 55

1 はじめに

ServerView Operations Manager(略して Operations Manager) は、Fujitsu ServerView Suite の無償のサーバ管理モジュールです。Windows および Linux(SUSE および Red Hat) で実行される業界標準サーバ、またはハイパーバイザ(VMware ESX/ESXi、Citrix XenServer、または Hyper-V) を使用する仮想マシン(VM) のホストとして動作するサーバの集中管理に使用されます。

1 つまたは複数の中央管理用サーバで、すべての物理サーバと仮想サーバを標準化した方法で管理します。中央管理用サーバには、一般的な Web ブラウザと Java Runtime Environment が搭載された、ネットワーク内の任意のワークステーションからアクセスできます。

Operations Manager は、プロセッサ、RAM、ハードディスク、ファン、電源などの重要なハードウェアコンポーネントを含めた個々のシステムを管理します。消費電力を監視して制御し、パフォーマンスと使用率のデータを分析して、サーバ構成を更新します。

Operations Manager のセキュリティコンセプトには、役割ベースのユーザ管理が含まれおり、3 つのコンセプトを基礎としています。

- LDAP ディレクトリサービス(Lightweight Directory Access Protocol) によるグローバルユーザ管理
- 役割ベースのアクセス制御(RBAC)
- 中央認証サービス(CAS) に基づくシングルサインオン(SSO)

RBAC では、タスク指向の権限プロファイルを各役割に割り当てることにより、ユーザのセキュリティコンセプトとユーザの企業構造を合わせて調整することができます。

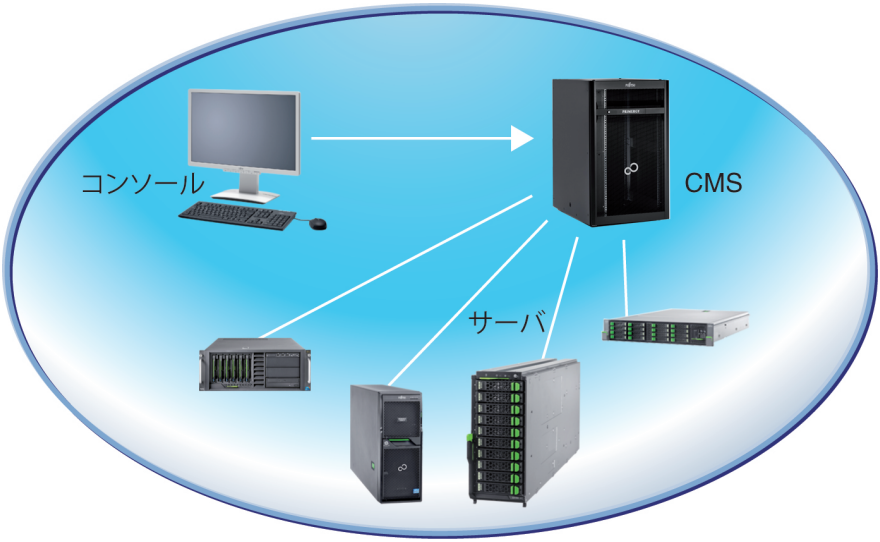
SSO によって、認証は 1 回だけで済みます。正常に認証されると、すべてのServerView コンポーネントへのアクセスが付与されます。再度サインオンする必要はありません。

Operations Manager によるサーバ管理は、サーバネットワークを総合的に管理するオペレータにとって重要な利点があります。

- サーバのフェールセーフによる、生産性の向上
- IT インフラストラクチャの自動監視機能によるコストの削減
- サーバは柔軟に拡張でき、Operations Manager は条件が変更されても簡単に調整可能
- シンプルなエラー分析によるダウンタイムの短縮
- エネルギー効率を確保し、可能な場合はサーバを無人操作
- エラー発生時の対応時間を短縮
- ネットワークコンポーネントおよびそのリソースを効率的に使用することで、総所有コスト(TCO) を削減
- 分かりやすいデータ表示、高機能なユーザインタフェース、支援的ヘルプシステムによる高い操作性

1.1 アーキテクチャ

ServerView Operations Manager のアーキテクチャは、管理コンソール、管理用サーバ(CMS) 、監視対象サーバに基づいています。



	管理コンソール ブラウザベースのコンソールでサーバを管理でき、指定したデータを表示することができます。ブラウザとして以下を使用できます。 ● Internet Explorer V9/V10 がインストールされている Microsoft Windows または Mozilla Firefox V16/V17 ● Mozilla Firefox V16/V17 がインストールされている SUSE/Red Hat Linux Java Runtime Environment のインストールも必要です。
	中央管理用サーバ(CMS) 管理用サーバ(CMS) には、ServerView Operations Manager のインストールが必要です。Virtual IO-Manager などの ServerView Suite のオプションコンポーネントも管理用サーバにインストールされ、Operations Manager に統合されます。 ServerView が作成して使用するデータは、SQL Server 内の SQL データベースに保存されます。以下の SQL Server が ServerView Operations Manager のインストールに含まれます。 ● Windows Server : SQL Server 2008 R2/2005 Express ● Linux Server : PostgreSQL 管理用サーバには Java Runtime Environment が必要です。 ServerView Operations Manager のインストール手順については、次のマニュアルを参照してください。 ● Installing ServerView Operations Manager Software under Windows ● Installing ServerView Operations Manager Software under Linux

	管理対象サーバ 管理対象サーバには ServerView エージェントまたは CIM プロバイダをインストールする必要があり、これによって中央管理用サーバに情報を提供します。ServerView RAID Manager および ServerView Update エージェントも管理対象サーバにインストールする必要があります。 仮想マシン(VM) への ServerView エージェントのインストールはリリースされていません。 ● ServerView エージェントは Windows、Linux、VMware ESX、Citrix XenServer で使用できます。 ● CIM プロバイダは VMware ESXi で使用できます。 ● Windows向けの ServerView CIM プロバイダは、ServerView エージェントをインストールすることで利用できます。現在、ServerView CIM プロバイダは ServerView Operations Manager でサポートされていません。 CIM プロバイダのインストール手順については、次のマニュアルを参照してください。 ● Windows の ServerView エージェント ● Linux の ServerView エージェント ● Installing ServerView ESXi CIM Provider ● Windows の ServerView CIM プロバイダ

1.2 本マニュアルの対象者および目的

本マニュアルは、ハードウェアおよびソフトウェアについての十分な専門知識をお持ちのシステム管理者、ネットワーク管理者、およびサービス技術者を対象としています。本マニュアルは、Linux SUSE、Red Hat、VMware、Citrix XenServer での ServerView エージェントのインストールについて説明しています。

1.3 技術的要件

1.3.1 最終段階での変更や修正

技術的要件の最終段階での変更や修正は、ServerView Suite DVD 1 に収録されている Readme ファイルに記載されています。以下のオプションがあります。

ServerView Operations Manager

- DVD 1 で、**SVSSoftware** – **Software** – **ServerView** – **[Windows | Linux]** – **ServerView_S2** ディレクトリに移動します。
- DVD 1 を起動し、「Welcome」ダイアログで次の順に選択します。**ServerView Software Products** – **実行**。**ServerView** – **Operations Manager** – **Info** マーク。

ServerView エージェント

- DVD 1 で、**SVSSoftware** – **Software** – **ServerView** – **[Windows | Linux]** – **Agents** ディレクトリに移動します。
- DVD 1 を起動し、「Welcome」ダイアログで次の順に選択します。**ServerView Software Products** – **実行**。**ServerView** – **Agents and Providers** – Info マーク。

1.3.2 管理コンソール

- http にアクセスできる標準的な PC/LAN
- Internet Explorer V9/V10 がインストールされている Microsoft Windows
- Mozilla Firefox V16/V17 がインストールされている Red Hat/SUSE Linux
- Java 7 Update 7 (バージョン 7.0.7) または JRE 1.6.0_35

1.3.3 中央管理用サーバ(CMS)

ハードウェア

- PRIMERGY サーバ
- PRIMEQUEST の場合のみ : PRIMEQUEST サーバ
- プロセッサのコア数:2以上
- メモリ:4GB以上
- LAN:100MBit-LAN
- 空きディスク容量:100 GB以上
- ディスプレイ 1280x1024(推奨、最小 1024 x 768)

ソフトウェア

- Windows
  - Microsoft Windows® Server 2012 の全エディション
    (ただし Server Core インストールなし)
  - Microsoft Windows® Server 2008 の全エディション
    (ただし Server Core インストールなし)
  - Microsoft Windows® Server 2008 R2 の全エディション
    (ただし Server Core インストールなし)
- Linux
  - Novell(SLES 10) : SP3 および SP4
  - Novell(SLES 11) : SP1 および SP2
  - Red Hat RHEL 5.7 および 5.8
  - Red Hat RHEL 6.2 および 6.3

データベース - Windows

- Windows でローカルマシンのデータベースを使用する場合:

  ServerView パッケージに付属 : SQL Server 2008 R2 Express SP2 および SQL Server 2005 Express SP4

  その他のサポート対象 :

  - SQL Server 2005 Standard、Workgroup、Enterprise
  - SQL Server 2008 Standard、Workgroup、Enterprise、Express
  - SQL Server 2008 R2 Standard、Workgroup、Enterprise、Express
- Windowsでリモートマシンのデータベースを使用する場合：
  - SQL Server 2005 Standard、Workgroup、Enterprise
  - SQL Server 2008 Standard、Workgroup、Enterprise
  - SQL Server 2008 R2 Standard、Workgroup、Enterprise

データベース – Linux(ローカルとリモート)

- PostgreSQL 8.4.12(ServerView パッケージに付属)

Java Runtime Environment

- Java 7 Update 7(バージョン 7.0.7) または JRE 1.6.0_35

1.3.4 ServerView エージェント

ServerView エージェントは以下の製品で使用できます。

- Windows Server 2008
- Windows Server 2008 x64
- Windows Server 2008 R2
- Windows Server 2012 Datacenter
- Windows Server 2012 Standard
- Windows Server 2012 Foundation
- Windows Storage Server 2012 Standard
- Novell (SLES 10) : SP3 以降
- Novell (SLES 11)
- Red Hat RHEL 5.7 および 5.8
- Red Hat RHEL 6.2 および 6.3
- Citrix XenServer V6.0
- VMware ESX Server V4.0 以降

バージョン 4.0 の VMware ESXi Server を監視できます。詳細は、『VMware ESXi – Monitoring ESXi Systems with ServerView Suite』マニュアルを参照してください。

1.4 旧版からの変更点

本版のマニュアルは ServerView Operations Manager V6.12 に適用され、オンラインマニュアル『 ServerView agents 6.11 for Linux 』(2012 年 12 月版) の更新版です。

1.5 ServerView Suite リンク集

リンク集により、富士通は ServerView Suite および PRIMERGY サーバに関するさまざまなダウンロードや詳細情報を提供します。

ServerView Suite には、以下のトピックに関するリンクがあります。

- サポートデスク
- マニュアル
- 製品情報
- セキュリティ情報
- ソフトウェアのダウンロード

ダウンロードには以下が含まれます。

- ServerView Suite の現在のソフトウェアステータスおよびその他の Readme ファイル。
- ServerView Update Manager により PRIMERGY サーバをアップデートする場合、および ServerView Update Manager Express により個々のサーバをローカルでアップデートする場合の、システムソフトウェアコンポーネントの情報ファイルおよびアップデートセット。
- ServerView Suite のすべてのドキュメントの最新バージョン。

ダウンロードは富士通 Web サーバから無償で入手できます。

PRIMERGY サーバには、以下のトピックに関するリンクがあります。

- サポートデスク
- マニュアル
- 製品情報
- スペアカタログ

リンク集へのアクセス

ServerView Suite のリンク集へアクセスする方法はいくつかあります。

1. ServerView Operations Manager から。

   - 開始ページまたはメニューバーで「**ヘルプ**」-「**リンク**」を選択します。

   ServerView リンク集の開始ページが開きます。

2. ServerView Suite DVD 2 から、または 富士通マニュアルサーバで Server-View Suite のオンラインドキュメントの開始ページを使用する。

   次のリンクを使用して、オンラインドキュメントの開始ページにアクセスします。

   http://support.ts.fujitsu.com

   - 左側の選択リストで「**Industry standard servers**」を選択します。
   - メニュー項目「**PRIMERGY ServerView Links**」をクリックします。

   ServerView リンク集の開始ページが開きます。

3. ServerView Suite DVD 1 から。

   - ServerView Suite DVD 1 の開始ウィンドウで、「**Select ServerView Software Products**」を選択します。
   - 「**Start**」をクリックします。ServerView Suite のソフトウェア製品が表示されるページが開きます。
   - メニューバーで「**Links**」を選択します。

   ServerView リンク集の開始ページが開きます。

1.6 ServerView Suite のマニュアル

ServerView Suite のマニュアルは、各サーバシステムに付属の ServerView Suite DVD 2 に収録されています。

マニュアルはインターネットからも無料でダウンロードできます。インターネットのオンラインドキュメントは、http://manuals.ts.fujitsu.comの「**Industry standard servers**」リンクをクリックすると入手できます。

ServerView Suite にあるマニュアルの概要およびファイル構造については、ServerView Suite サイトマップを参照してください（**ServerView Suite – Site Overview**）。

1.7 表記規則

この マニュアルでは以下の表記規則を使用します:

表記	説明
⚠	データの損失やデバイスの損傷の可能性があるリスクを表示します。
ⓘ	追加関連情報とヒントを表示します。
太字	インターフェイス要素の名前を示します。
等間隔表示	パスおよびファイル名など、出力やシステム要素を示します。
太字の等間隔表示	キーボードを使用して入力するテキストを示します。
青字の文字列	関連するトピックへのリンクを示します。

表記	説明
ピンク字の文字列	既に表示したリンクを示します。
<abc>	実際の値と置き換える必要がある変数を示します。
[abc]	オプション(構文)を示します。
[key]	キーボード上のキーを示します。大文字のテキストを入力する場合、[Shift] キーを指定します。たとえば、A を入力する場合 [SHIFT] + [A] を押します。2 つのキーを同時に押す場合は、2 つのキーをプラス記号で連結して示します。

マニュアルおよび実際の画面

ServerView Suiteの画面はシステムに依存しているため、表示される詳細はシステムによって異なる場合があります。また、システム固有の差異は、メニューオプションとコマンドに関連している場合があります。画面は予告なく変更となる場合があります。その場合は各画面のヘルプを参照して下さい。

2 管理対象サーバでの構成

Operations Manager を開始する前に、管理対象サーバで以下の準備を行ってください。

- PRIMERGY のみ : 各管理対象サーバで BIOS で一定の設定を指定する必要があります。20 ページの BIOS およびファームウェアの設定を参照してください。

  各サーバで、設定を行う必要があります。 24 ページの サーバの設定を参照してください。

- ServerView には高度なセキュリティコンセプトが取り入れられています。エージェントをインストールする前に、セキュリティコンセプトに関する情報をよく調査して、セキュリティ要件に最適なコンセプトを選択してください。エージェントをインストールする前に、適切な調整を行う必要があります。26 ページの ServerView のセキュリティコンセプトで説明しています。

- 現在のオペレーティングシステムの SNMP サービスを、管理対象サーバおよび管理用サーバにインストールして設定する必要があります。そうしないと、管理用サーバでサーバを監視できなくなります。オペレーティングシステムに応じて、エージェントのインストールの前または後に、SNMP サービスを有効にする必要があります。30 ページの SNMPサービスの設定で説明しています。

- ServerView エージェントを管理対象の各サーバにインストールする必要があります。33 ページの ServerView エージェントのインストールを参照してください。

  仮想マシン(VM) への ServerView エージェントのインストールはリリースされていません。

- ServerView Update Manager では、ServerView Update エージェントを管理対象サーバにインストールする必要があります。このインストールについては、『ServerView Update Management』ユーザガイドに記載されています。

- 中央管理用サーバで ServerView Operations Manager を、IP アドレスではなく名前を使用してアクセスするように設定する場合、このアドレスを使用して監視対象サーバからアクセスできるか確認してください。この場合、可能であれば DNS を使用してください。DNS を使用できない場合は、適切な設定を監視対象サーバで **hosts** ファイルに行ってください。このファイルは、Linux システムの **/etc** ディレクトリにあります。

管理対象サーバへの追加インストール

- ServerView RAID Manager

  ServerView RAID Manager を使用すると、ハードディスクを管理できます。ServerView RAID Managerがインストールされていない場合、RAIDドライブおよび状態は確認できません。

  インストールについては、『RAID Management』ユーザガイドに記載されています。

2.1 BIOS およびファームウェアの設定

次の説明は、PRIMERGY にのみ有効です。

使用されているシステムボードに応じて、さまざまな PRIMERGY タイプがさまざまな BIOS バージョンで機能するため、BIOS セットアップの個々の設定と操作は、ここでは詳しく扱いません。

各 BIOS バージョンの詳しい説明は、該当の『BIOS Setup Utility』リファレンスマニュアルや、システムボードのテクニカルリファレンスマニュアルに記載されています。

サーバの起動時に、BIOS セットアップシステムで「**O/S Boot Timeout**」メニュー項目を「**Disabled**」に設定してください。「Disabled」に設定しないと、インストール中にシステムが再起動します。

「**O/S Boot Timeout**」メニュー項目を「**Enabled**」に設定できるのは、すべてのインストール(ServerView エージェントも含む) を完了した後でシステムを再起動する場合のみです。

Linux のインストール時に、ファイルシステムのチェックが行われるように「**O/S Boot Timeout**」の値が設定されているかどうかも確認してください。この値が正しく設定されていないと、システムファイルのチェック中にシステムが再起動します。

2.1.1 BIOS の設定

OS が起動するまで、サーバ管理ファームウェアがサーバを監視します。その後、エージェントと Operations Manager が監視機能を引き継ぎます。

サーバごとに BIOS の設定を変更する必要があります。

コンピュータを再起動して、起動段階の適切なタイミングで [**F2**] キー または [**DEL**] キーを押し、BIOS セットアップを呼び出します。

BIOS セットアップに入ったら、「**Server**」メニューを選択します。このメニューでは、サーバ管理に必要な設定を指定できます。

BIOS セットアップで「**Server**」メニューが表示されない場合は、サーバ管理機能を有効にする必要はありません。ただし、これは、個々のサーバ管理機能の明示的な制御権を与えられていないことも意味することに注意してください。

「**Server**」メニューに「**Server Management**」メニュー項目が含まれている場合、この項目を選択して「**Enabled**」に設定します。これで、サーバ管理機能が有効になります。その他のすべての設定を有効にするには、ここで値「**Enabled**」を選択する必要があります。

「**Server Management**」メニュー項目を使用できない場合は、個々の機能に対する制御権は一般的なリリースに左右されません。

「**Server**」メニューでは、以下のメニューを使用できます。

下記の一部のフィールドは、ハードウェアによっては使用できない場合があります。

O/S Boot Timeout

事前に定義した期間内(起動後) に OS がサーバ管理ファームウェアとの接続を確立できない場合にシステムを再起動するかどうかを指定します。この期間は、Operations Manager を使用して設定することもできます(『Operations Manager User Guide』の「ASR&R」の項も参照) 。

サーバの起動時に「**O/S Boot Timeout**」メニュー項目を「**Disabled**」に設定してください。「Disabled」に設定しないと、インストール中にシステムが再起動します。

Action

boot watchdog が動作した後に行う動作を指定します。

Timeout Value

「**O/S Boot Timeout**」が「Enable」になっている場合に、システムの再起動までの時間を指定します。

ASR&R Boot Delay

エラー(気温が高すぎるなど) が原因でシステムがシャットダウンした後のシステムの自動再起動までの時間を指定します。

Boot Retry Counter

サーバがシャットダウンのままとなるか、RemoteView が起動されるまでの間にサーバが OS の再起動を試行する回数を指定します。

Diagnostic System

「**Boot Retry Counter**」で設定したシステム再起動の回数に達したときに RemoteView を起動するかどうかを指定します。

Hardware Watchdog

サーバ管理 BIOS がハードウェアカウンタを特定の時間間隔内にリセットできない場合に、サーバを再起動するかどうかを指定します。

Next Boot uses

次回のブート時に RemoteView を起動するかどうかを指定します。

Temperature Monitoring

温度が上限値を超えた場合にシステムをシャットダウンするかどうかを指定します。

Memory Scrubbing

メモリをテストしてシングルビットエラーを除去するかどうかを指定します。

BIOS Runtime Logging

プロセッサ/メモリ/PCI エラーをエラーログファイルに保存するかどうかを指定します。

CPU ステータス

プロセッサを使用できるかどうかを指定します。

メモリステータス

特定のメモリモジュールの異常を識別できるようにします。異常と識別されると、これらのモジュールは、次回のシステム起動時に使用されません。

Console Redirection

システム上でターミナルを動作させるための設定を指定します。

RomPilot

RomPilot の設定を指定します。RomPilot は、ServerView Remote Management および Operations Manager の一部です。RomPilot は、LAN を使用して、リモートコンソールからシステム起動フェーズ(POST) および MS-DOS にアクセスできるようにします。

Storage Extension

グループ設定および通信バス(CAN バス) の設定を指定します(注 : **Storage Extension** は、一部のサーバでは使用できません) 。

2.2 サーバの設定

サーバを設定するためのさまざまな機能があります。これらの機能の一部は、すべての PRIMERGY サーバでサポートされ、その他は PRIMERGY サーバに搭載されたハードウェアおよびソフトウェアに応じて、特定のサーバでのみ使用できます。

サーバは以下のいずれかの方法で設定できます。

- Server Configuration Manager を使用して管理対象サーバ上でローカルに設定する

  Server Configuration Manager を使用して、ターゲットシステムの一般的なシステム動作を設定し、ターゲットシステムのリモート管理コンポーネント(iRMC または iRMC S2/S3) を設定できます。

  ServerView Installation Manager を ServerView Suite DVD 1 から起動した場合、Server Configuration Manager を「**Server Configuration Manager**」ボタンから開始できます。

  ターゲットシステムの PRIMERGY サーバタイプによっては、すべてのステップを実行する必要はありません。また、個々のステップの順序や、個々のステップの設定オプションは、システムによって異なります。

  個々のサーバ設定ダイアログステップの詳細は、Server Configuration Manager のオンラインヘルプを参照してください。

  ダイアログステップに関連するオンラインヘルプにアクセスするには、次の手順に従います。

  1. このダイアログステップを現在表示しているウィンドウの領域をクリックします。
  2. F1 キーを押します。

- Operations Manager のグラフィカルユーザインターフェースに統合された ServerView Configuration Manager によって設定する。これにより、Web インターフェースを使用してリモートワークステーションからサーバを設定できます。

ServerView Configuration Manager を、Operations Manager の開始ページから、または「**管理者設定**」－「**サーバの設定**」を選択してメニューバーから開始します。

詳細については、ServerView Operations Manager のユーザガイドを参照してください。

ServerView エージェントがインストールされているサーバのみ設定できます。

システムによっては、指定された設定の一部が BIOS に書き込まれます。

以下のことを実行できます。

- サーバ、システムボード、iRMC の重要なデータを読み取ります。
- BOOT およびソフトウェアウォッチドッグの設定を読み取り、設定します。
- メモリモジュールのエラーカウンタを読み取り、編集します。

PRIMERGY のみ :

- サーバのエラーとイベントログを読み取り、削除します。
- システムファンを監視し、キャリブレーションを行います。
- シャーシ ID(出荷時に設定済み) を読み取り、設定します。
- システムランタイムのカウンタを読み取り、設定します。
- HTTP および Telnet の設定と、HTTP のリモート管理コントローラの設定を指定します。
- RSB Web インターフェースの IP および DNS 設定を指定します。
- リモート管理コントローラの SNMP インターフェースに対する SNMP コミュニティおよびトラップターゲットを指定します。
- リモート管理コントローラのユーザ ID を管理します。
- RSB とリモート管理コントローラのシリアルインターフェースを設定します。
- Operations Manager UPS 管理統合を設定します。
- ServerView Local Service Display のディスプレイに表示される情報を設定します。

2.3 ServerView のセキュリティコンセプト

ServerView SNMP エージェントと ServerView Manager は、サーバ上での不正な SNMP SET 操作を防止するセキュリティコンセプトを提供します。

管理対象サーバでの SNMP SET 操作へのアクセスを制限できます。以下のオプションがあります。

- 特定の SET 操作を禁止する。
- すべての SET 操作を禁止する。
- ユーザ認証によって SET 操作を保護する。

  ユーザ認証オプションを選択した場合、毎回SET 操作を開始する際にシステムはユーザ認証を実行します。認証ルーチンが正常に実行されると、システムは、ユーザが管理者によって定義されたユーザグループのいずれかに属しているか確認します。

  ユーザ認証は ServerView Manager でのみ動作します。その他の SNMP ツールでは動作しません。

SNMP サービスのデフォルト構成を変更することで、不正アクセスのリスクを低減することもできます。詳細は、30 ページの SNMPサービスの設定を参照してください。

2.3.1 特定の SET 操作の禁止

SET 操作によっては、システムがシャットダウンまたは再起動することがあります。これらの特別な SET 操作は許可することも禁止することもできます。46 ページの エージェントの設定の「AgentShut」を参照してください。

2.3.2 すべての SET 操作の禁止

ServerView エージェントのすべての SET 操作を禁止できます。エージェントのインストール時にこれらの仕様を入力します。46 ページの エージェントの設定の「AgentPermission」を参照してください。

このオプションは ServerView エージェントにのみ適用されます。その他の SNMP エージェントに対する SET 操作には影響はありません。

2.3.3 ユーザ認証による SET 操作

SET 操作へのアクセスを制限して、ユーザ認証によって SET 操作の実行を保護できます。ここでは、ユーザ認証ルーチンを管理対象サーバの各セッションの開始時に開始するか、または新規 SET セッションの開始時にユーザ認証を開始するかを、選択できます。

ユーザ認証については、管理対象サーバと管理用サーバで、以下の設定を指定する必要があります。

エントリ	設定
管理対象サーバ	• ユーザとユーザグループの定義 • 特定のユーザグループへのユーザの割り当て • エージェントのインストール中の指定されたユーザグループの指定
管理用サーバ	ユーザを Operations Manager の「**ログイン**」タブで指定します。

ユーザとユーザグループの定義と、ユーザの割り当て

各管理対象サーバで、オペレーティングシステムに固有の方法を使用して、ユーザとユーザグループを定義する必要があります。ユーザまたはユーザグループには任意の名前を選択できます（Administrator を含む）。

複数のサーバに同一のユーザとグループ ID を作成するかどうかを、事前に決定しておく必要があります。

エージェントのインストール中のユーザグループの指定

サーバへのエージェントのインストール中に、SET 操作の実行を許可されたユーザが属するユーザグループを指定する必要があります。ServerView エージェントのインストールと設定は、オペレーティングシステムとバージョンによって異なります。各条件でのインストールと設定の詳細につしては、46 ページのエージェントの設定以降のエージェントの説明を参照してください。

管理用サーバでのユーザの指定

管理用サーバでは、現在のサーバで SET 操作の実行を許可されているユーザを指定する必要があります。**サーバのプロパティ**ウィンドウの**ログイン**タブでユーザを定義します。以下の例ではユーザは**SVUSER**です。

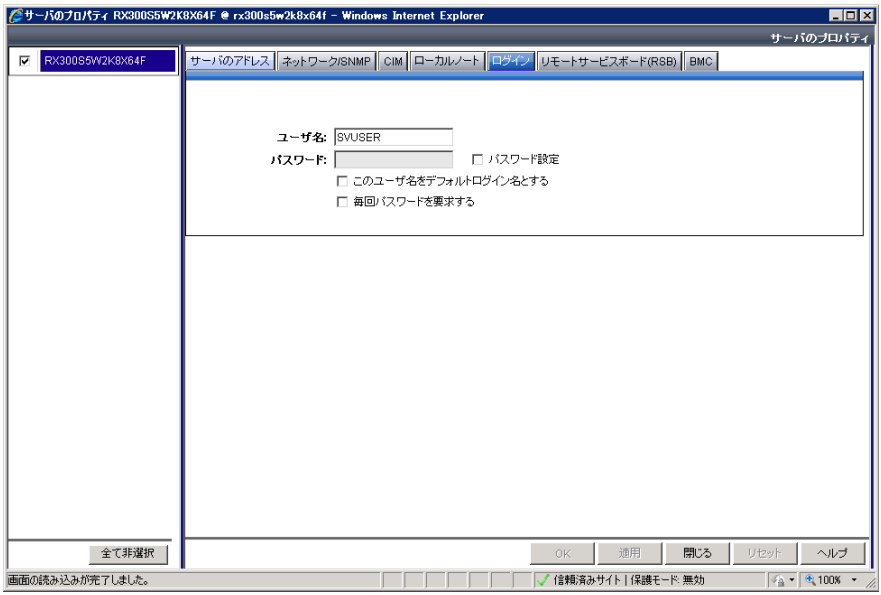


図 1: ユーザ認証のユーザ ID の定義

セキュリティ上の理由でユーザにパスワードを割り当てている場合は、ここにもパスワードを入力することを推奨します(**パスワードの設定**) 。「**毎回パスワードを要求する**」オプションでは、設定を変更するたびに、または Operations Manager を開始した後に初めて変更を行った後のみ、ユーザ名とパスワードを要求することを指定できます。「**毎回パスワードを要求する**」を有効にすると、パスワードが保存されないので、最高レベルのセキュリティを実現することができます。

「**サーバのプロパティ**」ウィンドウの左側で、設定を適用するサーバを選択できます。また、一度に複数のサーバを選択することもできます。これにより、各サーバにそれぞれ設定を適用するのか、または同じ設定を複数のサーバにまとめて適用するのかを指定できます。

以下の例では、ユーザ認証が有効な場合の手順を示します。

例

ユーザ **svuser** はサーバで設定され、管理用サーバの Operations Manager の「**ログイン**」タブで指定されています。管理用サーバを使用して SET 操作を実行すると、ユーザは識別情報の入力を求められます。

図 2: ユーザ認証

2.3.4 SNMP エージェントのオペレーティングシステム固有の特性

以降の項では、ServerView のセキュリティコンセプトの実現に関する、オペレーティングシステムおよびエージェントのバージョン固有の手順を説明します。

SNMP のセキュリティコンセプト

サーバを管理用サーバから監視するには、オペレーティングシステムをインストールした後に、**bin** グループに属するユーザを設定する必要があります。

該当する機能を有効にするには、このユーザ名と対応するパスワードを管理用サーバに入力する必要があります。

エージェントのインストール方法については、33 ページの ServerView エージェントのインストールを参照してください。

2.4 SNMPサービスの設定

現在のオペレーティングシステムの SNMP サービスを、管理対象サーバおよび管理用サーバにインストールして設定する必要があります。

ServerView Linux エージェントでは、システムの SNMP サービスの設定ファイルに設置パラメータを指定する必要があります。このファイルは /etc/snmp/snmpd.conf にあります。この設定ファイルは、vi などを使用して編集する必要があります。構文についての情報は、snmpd.conf のマニュアルページに記載されています(man snmpd.conf を呼び出す) 。

- sysContact に該当する連絡先を、sysLocation にサーバの場所を指定します。

  authtrapenable を 1(enable) に設定します。これにより、SET 操作中に管理用サーバのコミュニティが不明な場合、または SET 操作で必要な権限がない場合に、トラップが送信されます。2(disable) の場合、この機能を無効にできます(デフォルト) 。

  この詳細情報は、snmpd.conf のマニュアルページを参照してください。

- 以下の例では、ネットワークとサーバ環境を一致させるために調整する必要がある設定を示しています。

  ```
  com2sec svSec localhost public
  com2sec svSec <subnet>/<netmask> public
  group svGroup v1 svSec
  view svView included .1
  access svGroup "" any noauth exact svView none none
  ```

  環境に応じて <subnet>/<netmask> を調整する必要があります。デフォルトで、読み取り専用の SNMP アクセスが許可されています。

  3 つ以上の com2sec 定義を使用している場合は、順序が重要です。IP アドレスと受信 SNMP 要求のコミュニティに一致する最初の com2sec 定義が使用されます。このため、特定の IP 領域の com2sec 定義を、汎用アクセス用(同じコミュニティ) の定義の前に設定する必要があります。

subnet と netmask の構文など、詳細については、snmpd.conf のマニュアルページを参照してください。

- この例では、コミュニティ名は public です。

  セキュリティ上の理由で別のコミュニティ名を使用する場合は、例で使用されているコミュニティ名 public を選択した名前に置き換えます。

  選択したコミュニティ名を、「**サーバのプロパティ**」の「**ネットワーク/SNMP**」タブでも、管理用サーバに対して入力してください。

- SNMP アクセスによる値の変更は、デフォルトで許可されていません。管理用サーバで管理対象サーバの値を変更する、またはシャットダウンするには、SNMP SetRequests を許可する必要があります。このためには、上記の設定例の最終行を次のように変更します。

  ```
  access svGroup "" any noauth exact svView svView none
  ```

  AgentPermission と AgentShut の値が 3 に設定されていることも確認してください。これらの値の config ファイルでの定義の詳細は、46 ページの エージェントの設定を参照してください。

- SNMP トラップのターゲットアドレスを指定します。trapsink には、管理用サーバの IP アドレスまたは名前を入力します。複数の管理用サーバを入力できます。snmpd.conf に管理用サーバ 1 つにつき 1 行を追加します。

  ```
  trapsink <ホスト> <コミュニティ名>
  ```

  <コミュニティ名> には、public または使用するコミュニティ名を入力します。

- LSI/Mylex RAID コントローラの GAM エージェントは SNMP マスターエージェントと SMUX プロトコル(SNMP マルチプレックスプロトコル) を介して通信します。

  GAM エージェントがインストールされている場合、以下の行を SNMP 設定ファイルに追加する必要があります。

  ```
  smuxpeer .1.3.6.1.4.1.1608 mylex
  ```

- 変更を行った場合は、snmpd サービスまたはサーバを再起動します。

ファイアウォールがサーバで有効になっている場合、SNMP ポートが開いていることを確認してください。以下を受け付けることを確認してください。

- ポート 161(サービス名 snmp) 、プロトコル udp で受信パッケージ
- ポート 162(サービス名 snmptrap) 、トラップを送信できるプロトコル udp で送信パッケージ
- ポート 3172(リモートコネクタサービス) とポート 3173-(ServerView RAID Manager) 、tcp プロトコル

3 ServerView エージェントのインストール

3.1 要件

クライアント認証に PKI(Public Key Infrastructure) を使用する場合:

クライアント認証により、管理対象サーバが、信頼されない管理用サーバまたは管理用サーバで実行中の権限のないアプリケーションからアクセスされることを防ぎます。ServerView エージェントと共に証明書ファイルをインストールするか、ServerView エージェントがすでにインストールされている場合に管理対象サーバに証明書ファイルをインストールするかを、選択できます。

ServerView エージェントと共に証明書ファイルをインストールするには、エージェントを実際にインストールする前に、証明書ファイルがあらかじめ管理対象サーバにインストールされている必要があります。

詳細は、『ServerView でのユーザ管理』ユーザガイドを参照してください。

ServerView Operations Manager および ServerView RAID Manager に必要な追加パッケージについては、『Installation under Linux』インストールガイドに記載されています。

Citrix XenServer への ServerView エージェントのインストールは、XenServer サプリメント CD に収録されています。CD は ServerView Suite DVD 1(**ServerView - XenServer Supplements** または **SVSSoftware¥Software¥XenServer-Supplements**) に含まれています。ISO イメージを Fujitsu Technology Solutions の Web サーバ(http://-support.ts.fujitsu.com/com/support/downloads.html) からダウンロードすることもできます。必要なソフトウェアパッケージ、インストールをサポートするスクリプト、設定およびリリース文書が含まれています。

VMware ESX Server サプリメントは ServerView Suite DVD 1(**ServerView - VMware Supplements** または **SVSSoftware¥Software¥VMware-Supplements**) に含まれています。

- ServerView エージェントをインストールする前に、オペレーティングシステムプラットフォームに応じて、該当する **Net-SNMP** パッケージがインストールされていることを確認してください。

VMWare ESX	**net-snmp** および **net-snmp-utils**
SUSE SLES	**net-snmp**
Red Hat Enterprise Linux	**net-snmp** および **net-snmp-utils**
Citrix XenServer	**net-snmp**

- ServerView エージェントには、以下のソフトウェアパッケージが必要です。(32 ビットパッケージは 64 ビットアーキテクチャにも必要です):
  - SUSE SLES(パッケージの名称表記は SLES のバージョンとアーキテクチャによって異なります):

SLES10 SP3	**libstdc++33** および **openssl**
SLES V11	**libstdc++33** および **libopenssl0_9_8**

    64 ビットアーキテクチャでは、パッケージの末尾に **-32bit** が付いています。
  - Red Hat、VMware、Citrix XenServer:

    compat-libstdc++-33 および **openssl**
- ServerView System Monitor の追加要件
  - X11 ベースのグラフィカルデスクトップ環境。KDE と GNOME をサポートします。
  - 適切な Java Runtime Environment は V1.6.0_25 以降。ServerView Suite DVD 1 で提供される Java Runtime の使用を推奨します。日本語環境では、Java Runtime Environment V1.6.0_30 以上に対応します。
  - RAID 情報を表示するには、ServerView RAID Manager をインストールして実行する必要があります。
  - オンラインヘルプページを表示するには、Web ブラウザをインストールする必要があります。

- ServerView エージェントのカーネルモジュール

  Linux の ServerView エージェントは通常、他のカーネルモジュールに確立されたプロセスを使用して基礎となるシステムに提供される(ロード可能な) カーネルモジュールで動作します。

  最新の互換性のあるカーネルモジュールを提供するため、PLDP(- Partner Linux Driver Process(SLES 10)) と DUP(Driver Update Process(RHEL 5)) プログラムを使用できます。PLDP と DUP の詳細は、以下にアクセスしてください。

  http://ts.fujitsu.com/products/standard_servers/linux_readmes_popup.html

  これが失敗した場合や、PLDP または DUP をサポートしていないシステムの場合、Linux エージェントをインストールするには、ローダブルモジュールがすでにコンパイルされているか、またはソースコードからモジュールをコンパイルする必要があります。

  コンパイルを許可するには、カーネルのソースコード(**kernel-source** パッケージ) および GNU C 開発システムをインストールしてください(Citrix Xen Server および VMware の場合は除く) 。

  - SUSE SLES:

    SUSE SLES 10/11 のコンパイルには、**kernel.source<kernel version>.rpm** パッケージが必要です。

  - Red Hat:

    Red Hat には、**kernel-[<feature>-]devel-<release>** パッケージが必要です。

  自分で作成したカーネルを使用する場合、該当するインクルードファイルがサーバにあることを確認する必要があります。

- RAID 周辺機器の管理には、ServerView RAID Manager をシステムにインストールする必要もあります。インストールについては、『RAID Management』ユーザガイドに記載されています。
- ServerView Suite DVD 1 を挿入し、CD のルートディレクトリで、**start.html** ファイルを Web ブラウザで開きます。「**ServerView**」 – 「**Agents and Providers**」に移動して、表の中の「**ServerView Agents Linux and VMware** 」リンクをクリックします。

  「**Supported Systems**」にリリースされた PRIMERGY システムの一覧があります。
- CMOS クロックを GMT ではなくローカルタイムに設定する必要があります。設定しない場合、自動電源オン/オフ機能が設定した時刻に開始されません。ローカルタイムは各オペレーティングシステムで次のように設定されます。
  - VMware:

    hwclock – localtime コマンドを使用して、CMOS クロックにローカルタイムを割り当てます。
  - SUSE:

    YaST – System で、CMOS クロックにローカルタイムを割り当てます。

    SUSE SLES 11:

    以下の設定を確認します。

    「**Hardware Clock Set To UTC**」オプションを無効にする必要があります。

    「**Date and Time**」ウィンドウで、「**Local Time**」エントリを「**Hardware Clock Set To**」選択リストから選択します。
  - Red Hat:

    linuxconf で、CMOS クロックにローカルタイムを割り当てます。

    以下の設定を確認します。

    「**Date and Time Properties**」ウィンドウの「**Time Zone**」タブで、「**System Clock**」オプションを使用できます。

「System Clock uses UTC」オプションを無効にする必要があります。

「System」－「Administration」－「Date & Time」を選択します。

date コマンドを使用してシステム時間を出力し、hwclock --show を使用して CMOS 時間を出力します。時間が異なる場合は、hwclock コマンドを使用して CMOS 時間がシステム時間に一致するように変更します。hwclock コマンドの詳細は、hwclock --help を使用して参照できます。

- SLES10 および SLES11 のドライバ監視機能には、syslog-ng 設定ファイルの拡張が必要です。
  - SUSE SLES 10:
    1. 次の行をファイル /etc/syslog-ng/syslog-ng.conf.in に挿入します。

       ```
       destination hwlog { pipe("/dev/HWLog/syslog_
       fifo"); };
       ```

       ```
       log { source(src); destination(hwlog); };
       ```

    2. 次のコマンドを実行します。

       ```
       /sbin/SuSEconfig
       ```

  - SUSE SLES 11:
    1. 次の行をファイル /etc/syslog-ng/syslog-ng.conf に挿入します。

       ```
       destination hwlog { pipe("/dev/HWLog/syslog_
       fifo"); };
       ```

       ```
       log { source(src); destination(hwlog); };
       ```

  - SUSE SLES 10 および SUSE SLES 11:
    1. YaST を起動してNovell AppArmor － Edit Profileの順に選択します。
    2. アクティブな syslog デーモンの名前(/sbin/syslog-ng または /sbin/syslogd) を選択して「次へ」をクリックします。
    3. 「Enter 」または「modify Filename」フィールドに /dev/HWLog/syslog_fifo と入力します。
    4. PermissionsでRead and Writeオプションを有効にします。

5. この入力を保存します。
6. 次により AppArmor を再起動します。

   ```
   /etc/init.d/boot.apparmor restart
   ```

7. 次により syslog サービスを再起動します。

   ```
   /etc/init.d/nldap restart
   ```

- Red Hat および VMware におけるドライバ監視機能：

  インストール時に次の行が **syslog** デーモンコンフィギュレーションファイルに挿入され、**syslog** デーモンが再起動されます。

  ```
  *.info;mail.none;news.none;authpriv.none;cron.none
  |/opt/fujitsu/ServerViewSuite/HWLog/path/syslog_
  fifo
  ```

  アンインストール時にこのエントリは削除され、**syslog** デーモンが再起動されます。

  Red Hat の場合は、syslog デーモンの **syslog**(Red Hat5) または **rsyslog**(Red Hat5.6、Red Hat6) をインストールできます。

  syslog 設定ファイルを変更する手順では、**rsyslog** デーモン設定ファイルおよびこのデーモンの再起動が好まれます。**syslog** デーモンを使用する場合は、**rsyslog** をインストールしないでください。

- SELinux 機能を無効にしてください(Red Hat バージョン 6.0 では不要) 。

3.2 スクリプトベースのインストール

srvmagt スクリプトを使用して ServerView エージェントをインストールします。このスクリプトは、これまでの蓄積からわかるすべての依存をテスト/検証し、必要なすべての準備を把握してから、必要なアクションを実行して、ServerView Agents Linux をシステム上に確立しようとします。

このスクリプトは以下のことを実行します。

- Linux 配布(SUSE、Red Hat など) を識別する。
- カーネルのバージョンおよびアーキテクチャ(x86、x86-64、または ia64) を識別する。
- BIOS データを使用して PRIMERGY サーバのモデルを識別する。
- PLDP(Partner Linux Driver Process) および DUP(Driver Update Process) がサポートされているかどうかを識別する。この場合、必要に応じて、スクリプトは ServerView カーネルモジュールパッケージ(KMP) を自動的にインストールしようとします。
- SNMP パッケージ、および特定のモデルまたはディストリビューション用のその他のパッケージの存在を確認します。
- **snmpd.conf** の設定(日本語 OS 環境の場合のみ)

  日本語 OS で ServerView エージェントをインストールすると、インストールスクリプトによって SNMP サービスを設定する必要があるかどうかがチェックされます。必要がある場合、バックアップファイル **/etc/snmp/snmpd.conf_svsave** が作成され、以下のエントリがファイル **/etc/snmp/snmpd.conf** に追加されます。

  ```
  com2sec svSec localhost public
  com2sec svSec 127.0.0.1 public
  com2sec svSec default public
  group svGroup v1 svSec
  view svGroup included .1
  ```

```
access svGroup "" any noauth exact svView svView
none
trapsink 127.0.0.1
```

詳細については、30 ページの SNMPサービスの設定を参照してください。

3.2.1 ServerView Suite DVD 1 を使用したインストール

ServerView Suite DVD 1 には、ServerView エージェントとシェルアーカイブ **srvmagtDVD.sh** の rpm パッケージが収録されています。ServerView Suite DVD 1 の次のディレクトリにスクリプトが格納されています。

SVSSoftware – Software – ServerView – Linux – Agents

エージェントをインストールするには、次の手順に従います。

1. ServerView Suite DVD 1 を挿入し、必要に応じてマウントします。
2. 次のディレクトリに変更します。

   SVSSoftware – Software – ServerView – Linux – Agents
3. インストールスクリプト **srvmagtDVD.sh** を **/tmp** に保存します。
4. ターミナルを(ルートで) 開きます。
5. **/tmp** ディレクトリに切り替えます。

   ```
   cd /tmp
   ```
6. 次のコマンドを入力します。

   ```
   srvmagtDVD.sh [-R] [--ssm install | not-install]
   ```

   -R

   他の RPM パッケージとともに ServerView RAID Manager RPM パッケージが提供されている場合は、インストールします。

   --ssm install | not-install

   ServerView System Monitor のインストールを指定します。デフォルトでは、ServerView System Monitor をインストールします。

   このオプションは、Red Hat または SUSE システムでのみ評価されます。

これで、スクリプトによりインストールが自動的に実行されます。

ServerView System Monitor のインストールが失敗しても、ServerView エージェントのインストールは中断されません。

3.2.2 ディレクトリからのインストール

Fujitsu Technology Solutions の Web サーバから任意のディレクトリにスクリプトをダウンロードすることもできます。

エージェントをインストールするには、次の手順に従います。

1. インストール RPM パッケージとシェルアーカイブ **srvmagt.sh** を任意のディレクトリに保存します。
2. ターミナルを(ルートで) 開きます。
3. 該当ディレクトリに切り替えます。

   ```
   cd <path>
   ```

4. 次のコマンドを入力します。

   ```
   ./srvmagt.sh [option] install
   ```

   オプションについては、43 ページの srvmagt スクリプトで説明しています。

このスクリプトは、すべての RPM パッケージをインストールします。

3.3 rpm コマンドを使用するインストール

rpm コマンドを使用してインストールするには、以下の手順に従います。

1. ターミナルを(ルートで) 開始します。
2. ServerView Suite DVD 1 をマウントします。

   ```
   mount -t udf -o loop /dev/cdrom /mnt/cdrom
   ```

3. Linux エージェントを含むディレクトリに移動します。

   ```
   cd /mnt/cdrom/SVSSof-
   tware/Software/ServerView/Linux/Agents
   ```

4. 以下の RPM パッケージをインストールします。

   ```
   rpm -U ServerViewConnectorService-<scs-
   version>.i386.rpm
   rpm -U srvmagt-mods_src-<version>.i386.rpm
   rpm -U srvmagt-eecd-<version>.i386.rpm
   rpm -U srvmagt-agents-<version>.i386.rpm
   rpm -U SVSystemMonitor-<version>.i386.rpm
   ```

   パッケージは上記の順序でインストールしてください。

   <scs-version>
   Remote Connector Service のバージョンおよびリリース番号(1.12.00 など) を指定します。

   <version>
   ServerView Linux エージェントのバージョンおよびリリース番号(6.11-04 など) を指定します。

3.4 エラーの考えられる原因

- コンパイル中にエラーが発生した場合、適切なカーネルソースコードがサーバ上にないことが考えられます。
- 続けてモジュールのコンパイルを手動で開始するには、以下のコマンドを使用します。

  ```
  /etc/init.d/eecd_mods_src start
  ```

  コンパイラの出力を表示するには、ディレクトリ **/etc/srvmagt/sources** で make を直接開始します。

3.5 インストール後の ServerView エージェントのメンテナンス

3.5.1 srvmagt スクリプト

40 ページの ServerView Suite DVD 1 を使用したインストール、または 41 ページの ディレクトリからのインストールに記載されているように ServerView Agent for Linux をインストールすると、**srvmagt** スクリプトを使用して管理するための追加機能が提供されます。

1. ターミナルを(ルートで) 開きます。
2. コマンドを入力します。構文を参照してください。

構文

```
[/usr/sbin/]srvmagt [option] [action]
```

option には、以下を指定できます。

–f

発行された警告/拒否に対して、目的のアクションを強制します。

その場合、ユーザは自身のリスクと責任に基づいて決定を下してください。動作と機能は定義されていません。

-h | --help

コマンド構文を表示して終了します。

-n

インストールアクションによるインストール中に、いかなる ServerView エージェントのデーモンも起動しません。

-p <path>

ここで、RPM パッケージが含まれているディレクトリを指定できます。

<path> は、ローカル/リモートファイルシステムのディレクトリへのパスです。

このパスオプションには、スペースまたは特殊文字は使用しないでください。

-R

他の RPM パッケージとともに ServerView RAID Manager RPM パッケージが提供されている場合は、インストールします。

--ssm install | not-install

ServerView System Monitor のインストールを指定します。デフォルトでは、ServerView System Monitor をインストールします。

このオプションは、Red Hat または SUSE システムでのみ評価されます。

-v <vers>

処理するバージョンを指定します。デフォルトは、スクリプトのバージョンです。

--version

スクリプトのバージョンを表示して終了します。

-V

verbose 情報を表示します。

action(アクション)として、以下を指定できます。

install

すでにインストールされている設定、および -v オプションで指定されたバージョンに従って、すべての ServerView Agents Linux の RPM パッケージをインストール(修正、アップデート) します。-n オプションも指定されていない場合は、該当のサービス(つまり、デーモン) が後で起動されます。

start

ServerView Agents Linux を起動します。

restart

ServerView Agents Linux を再起動します。

status

ServerView Agents Linux のステータスを表示します。

diag

PrimeCollect(8) を呼び出して、診断材料を収集します。

stop

ServerView Agents Linux を停止します。

remove

すべての ServerView Agents Linux の RPM パッケージを削除します。

オペレーティングシステムが Citrix XenServer の場合、ServerView RAID パッケージも同時に削除されます。

3.5.2 エージェントの設定

/etc/srvmagt/config ファイルには、管理対象システムへのアクセスを制限し、その他の運用パラメータを選択できる情報が含まれています。

「#」で開始する行はコメント行で、その他の行は次の形式です。

<キーワード>=<値>

AgentPermission	他のシステムが SNMP コマンドを使用してローカルサーバの値を設定するための基本アクセス許可です(2:許可しない、3:許可する、デフォルト:2(日本語 OS 環境の場合のデフォルト:3))。SNMP SetRequest を許可する場合は、この値を 3 に設定し、SNMP サービスを適切に設定します(30 ページの SNMPサービスの設定を参照)。
AgentShut	SNMP コマンドを使用して、ローカルサーバをリモートでシャットダウン/リブートするためのアクセス許可です(2:許可しない、3:許可する、デフォルト:2(許可しない)(日本語 OS 環境の場合のデフォルト:3))。SNMP SetRequest を許可する場合は、この値を **3** に設定し、SNMP サービスを適切に設定します(30 ページの SNMPサービスの設定)。
ShutdownDelay	SNMP シャットダウン要求とシャットダウンとの間の遅延(分単位)を示します。
NoAccountCheck	このエントリに 0 以外の値が指定されている場合、設定を ServerView で変更するときにパスワードを求められません。デフォルト値は 0 で、ユーザグループ認証がデフォルトで有効になっています。この場合、ユーザグループは「**UserGroup**」に入力する必要があります。ここには、SNMP 設定を変更するユーザが属する必要があります。 無効にされたパスワードの照会によって、セキュリティ上のリスクが生じることに注意してください。

UserGroup	**NoAccountCheck** に 0 が指定されている場合、Operations Manager では SNMP 設定を変更するために管理用サーバのユーザ/パスワードの組み合わせが要求されます。ユーザにアクセス権を許可するには、ユーザが **UserGroup** に指定されたユーザグループに属している必要があります。デフォルト設定は **bin** で、**root** が含まれています(日本語 OS 環境ではデフォルト設定は **svagtuser**) 。 ここで指定されたユーザグループが存在しない場合、オペレーティングシステム固有のリソースを使用して作成する必要があります。
ScanTapeDevices	これが 0 以外の値に設定されている場合、テープデバイス **/dev/nst*** が開き、現在のステータスを取得できます。テープデバイスが開くと、読み書き位置が意図せずに変更されることがあります(ドライバによる) 。テープデバイスがサーバ間で共有されている場合、このパラメータは Operations Manager がテープ操作(バックアップなど) に影響しないようにします。デフォルトはゼロで、テープデバイスは開きません。
TraceFileLimit	**/var/log/srvmagt** に保存されるトレースファイルのサイズを制御します(1 がデフォルト値で約 200 MB のスペースを必要とします。0 はトレースファイルなし、2 は約 400 MB の特大のトレースファイルを意味します) 。
InventoryRescan	サーバのインベントリデータが更新される時間(分単位) を指定します。デフォルト値は 120 です(日本語 OS 環境のデフォルト値は 0 です) 。1 ～ 120 の値は、120 に設定されます。値 0 の場合、更新は無効にされます。

config ファイルへの変更は、エージェントを再起動しないと反映されません。このためには、サーバを再起動するか、次のコマンドをシステム管理者として実行します。

```
/usr/sbin/srvmagt restart
```

VMware ESX、Citrix Xen または Xen

ServerView Operations Manager で VMware ESX、Citrix Xen、または Xen に対してパフォーマンスマネージャおよびスレッシュホールドマネージャをサポートするには、ServerView VME エージェント内のシステムに対してアカウント情報を設定する必要があります。それには、次の手順が必要です。

1. **/etc/srvmagt/VME/etc/app.config.xml ファイルを編集します**。
2. **<authentication>** というタイトルの項を検索します。
3. 必要に応じてユーザ情報とパスワード情報を入力します(たとえば、**<User>us123</User><Password>123passwd</Password>**) 。

   パスワードはプレーンテキストなので、このファイルへのアクセスを制限する必要があり、特権ユーザを使用しないでください。

4. ファイルを保存します。
5. ServerView エージェントを再起動します。

KVM 仮想ホストでは、ユーザ名とパスワードは不要です。

3.5.3 ServerView エージェントの改善された可用性

ServerView エージェントの開始スクリプト **srvmagt(8)** は、srvmagt cron スクリプト **srvmagtCron** を呼び出して 15 分ごとに動作します。

srvmagtCron は、eecd デーモン、ServerView エージェント、**SVRemoteConnector**、SNMP デーモン **snmpd** をチェックして、動作していなければ再起動します。また、個々のチェック時間を **/var/log/srvmagt/log.srvmagtCron** ファイルの最初の行に書き込みます。

srvmagt(8) で ServerView エージェントを停止すると、この定期監視は停止されます。

ルートの crontab から **srvmagtCron** を削除することはできません。影響を受けやすい crontab の変更を最小限に抑えるためです。実際の実行は、**srvmagt** ルートディレクトリ内の **srvmagtCronOn** ファイルの存在によって異なります。このファイルは ServerView エージェントの起動中に作成され、エージェントが停止されると削除されます。

3.5.4 ServerView エージェントのアンインストール

サーバの BIOS に保存された項目は、ServerView エージェントをアンインストールしても元の状態に戻りません。設定を元の状態に戻してから、ServerView エージェントをアンインストールしてください。ServerView エージェントをアンインストールする前に、以下のことを必ず行ってください。

1. ソフトウェアウォッチドッグ、BOOT ウォッチドッグ、電源 ON/OFF 設定を無効にしてください。
2. パフォーマンスマネージャでしきい値監視およびレポート作成を適用している場合は、サーバへの適用を解除してください。
3. ServerView エージェントのアンインストール時に、ServerView Operations Manager を使用して設定される設定値(電源スケジュールや ASR 設定など)は削除されます。設定を自動的に引き継ぐオプションはないため、アンインストール前に設定値をコピーしておいてください。そうしないと、アップデートインストールの後に再設定が必要になります。

ServerView エージェントをアンインストールするには、以下のコマンドを入力します。

```
/usr/sbin/srvmagt remove
```

Citrix XenServer では、ServerView RAID Manager もこのコマンドを使用してアンインストールされます。

3.5.5 ServerView エージェントの開始と停止

Linux エージェントがインストールされた後、エージェントはシステム起動時に自動的に開始します。診断のためには、エージェントを明示的に停止して再起動すると有効です。

エージェントの開始

以下のコマンドでエージェントを開始します。

```
/usr/sbin/srvmagt start
```

Linux エージェントを開始する前に、SNMP マスターエージェント **snmpd** を開始してください。

エージェントの停止

以下のコマンドでエージェントを停止します。

```
/usr/sbin/srvmagt stop
```

3.5.6 補足情報

- S30 または S40 が SCSI(SAF-TE) でサーバに接続され、エージェントによって登録されていない場合は、Linux で設定されるデバイスファイルが不足していることがあります。これらのデバイスファイルは SNMP エージェントとストレージ拡張ユニットの通信に必要です。デフォルトで、Linux は SCSI 接続に **/dev/sg0** から **/dev/sg15** まで 16 個までのデバイスファイルを設定します。17 台以上のデバイスを SCSI を接続するには、追加のデバイスファイルを指定する必要があります。SCSI デバイスファイルの数は、**/proc/scsi/scsi** ファイルに指定されています。追加のデバイスファイル(**/dev/sg**) は、以下のコマンドを使用して追加できます。

  ```
  mknod /dev/sg<番号> c 21 <番号>
  ```

  <番号> には、最後にあるエントリに続く番号を入力します(たとえば、最後のエントリ番号が 15 の場合、16 から始まる番号) 。新しいデバイスファイルを作成した後、サーバを再起動する必要があります。

- 新しいハードウェア(リモートサービスボードなど) を取り付けたり、新しいストレージ拡張ユニットを追加しても、認識されない場合は、**eecd**(environment enclosure control daemon) の「再スキャン」の実行が必要になります。次のコマンドを使用して **eecd** を再起動します。

  ```
  /etc/init.d/srvmagt stop
  /etc/init.d/eecd stop
  /etc/init.d/eecd rescan
  /etc/init.d/srvmagt start
  ```

3.5.7 管理ユーザの設定

ServerView の**管理者**権限を持つグループに属するユーザのみ、ServerView Operations Manager から監視対象サーバの ASR(Automatic Server Reconfiguration & Restart) 設定(ファン/温度/再起動設定など) やサーバのシャットダウンなどの操作を行うことができます。これらの操作には管理者ユーザの名前とパスワードが必要です。

管理者権限のあるグループは **UserGroup** に設定されているグループです。46 ページの エージェントの設定を参照してください。

管理者ユーザを設定するには、次の手順に従います。

- 新規ユーザを管理者ユーザとして作成します。

  root としてログインして、以下のコマンドを実行します。

  1. **useradd** コマンドの **G** オプションに**管理者権限を持つグループ名**を指定します。

     # useradd -G <管理者権限を持つグループ名> <ユーザ名>

     # passwd <ユーザ名>

     <ユーザ名> には、作成するユーザの名前を指定します。

  2. **passwd** コマンドを使用して新規ユーザのパスワードを設定します。確認のためにパスワードは 2 回入力する必要があります。

  パスワードを設定すると、新規作成したユーザ名が有効になります。コマンドの詳細については、**useradd** (8) および **passwd** (1) の man ページを参照してください。

- 既存のユーザを管理者ユーザとして設定します。

  設定しようとしている既存のユーザが複数のグループに属していないかどうかをシステム管理者に確認してから、次のコマンドを実行します。

ユーザがメイングループにのみ属している場合：

```
# usermod -G <管理者権限を持つグループ名> <ユーザ名>
```

ユーザが複数のループに属している場合：

```
# usermod -G <管理者権限を持つグループ名>,<ユーザグループ,...> <ユーザ名>
```

usermod コマンドの G オプションに管理者権限を持つグループ名を指定します。複数のグループを指定するには、グループをカンマ ″,″ で区切ります。ユーザがあらかじめ属しているグループを指定しないと、ユーザはそのグループから削除されます。ユーザが属しているグループをすべて指定してください。

<ユーザ名> に、管理者ユーザとしてユーザ名を指定します。

usermod コマンドの詳細については、usermod (8) man ページを参照してください。

またグループは、vigr コマンドを使用して直接設定することも、GUI ツールを使用して設定することもできます。詳細については、vigr (8) man ページまたは Red Hat Linux のマニュアルを参照してください。

3.5.8 インストール後のコンピュータ情報の変更

管理用 ServerView Linux エージェントがインストールされているサーバのコンピュータ名または IP アドレスを変更する場合、ServerView Linux エージェントで設定などを変更する必要はありません。

ただし、個々の環境の snmpd.conf ファイルを以前編集したことがある場合は、必要に応じて snmpd.conf ファイルを編集します。

snmpd.conf ファイルを編集したら、snmpd サービスと ServerView Linux エージェントを次の手順で再起動します。

1. root としてログインします。
2. 次のコマンドを実行します。

```
# /usr/sbin/srvmagt stop
# /etc/init.d/snmpd stop
```

```
# /etc/init.d/snmpd start
# /usr/sbin/srvmagt start
```

3.5.9 アップデートインストール/カーネルのアップデート

このセクションでは、ServerView Linux エージェントのアップデートインストールプロセスについて説明します。

1. ソフトウェアウォッチドッグと BOOT ウォッチドッグを **Enable** に設定している場合は、**Disable** に設定します。
2. カーネルアップデートを使用してカーネルをアップデートして、OS をリブートします。
3. **/etc/snmp/snmpd.conf_svsave** ファイルが作成されます(日本語環境のみ) 。

   /etc/snmp/snmpd.conf_svsave ファイルの存在を確認します。

   このファイルが存在しない場合、次のコマンドで作成します。

   ```
   # cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf_
   svsave
   ```

   snmpd.conf ファイルが存在する場合、インストールスクリプトで編集されません。
4. ServerView Linux エージェントをアップデートします。
5. 手順 1 でソフトウェアウォッチドッグと BOOT ウォッチドッグを無効にした場合は、有効に戻します。

3.5.10 パフォーマンスマネージャによるレポートの出力

パフォーマンスマネージャのレポート設定で、レポートの出力を有効にします。

レポートデータの保存

レポートデータは次のフォルダに保存されます : /var/srvmagt/reports/

レポートデータのファイル

以下のファイルが各レポートに作成されます。xxx は、パフォーマンスマネージャに設定されているレポート名を示します。

- xxx.dat
- xxx.ind
- xxx.names

パフォーマンスマネージャでレポート設定を削除すると、これらのファイルも削除されます。

パフォーマンスマネージャのレポートの定義で記録するレポートの最大エントリ数を設定しない場合や、短い間隔でサーバをポーリングして長時間レポートを出力した場合、ファイルサイズが大きくなりすぎるためディスク容量が制約されてしまうことがあります。これを回避するには、エントリ数とレポートを出力する間隔を正しく設定します。

3.5.11 /tmp ディレクトリ配下の一時ファイル

ServerView Linux エージェントを起動すると、S.xxxxxx(xxxxxx は任意のアルファベット文字列) という名前の、サイズがゼロバイトの一時ファイルが /tmp ディレクトリに作成されます。

このファイルにより、ServerView エージェントのサブエージェントと snmpd が通信できます。

このファイルの場所は変更できません。

また、このファイルを手動で削除すると、ServerView Linux エージェントが正常に動作しなくなる場合があります。

3.5.12 syslog のソース名

ServerView エージェントがハードウェアエラーを検出すると、エラーが syslog に記録されます。ServerView エージェントが報告するイベントのソース名は、**Serverview** です。

3.6 APC UPS の設定

次の説明は、PRIMERGY にのみ有効です。

UPS を監視するためには、対応するエージェント(APC) をサーバにインストールする必要があります。Web カード付きの APC UPS の場合、該当する SNMP エージェントが Web カードにあらかじめインストールされています。

既存の UPS 構成を Operations Manager アプリケーションに表示するには、先にインストールプログラムから入力しておく必要があります。UPS の自動検出はまだ実装されていません。そのため、UPS の各エントリには監視対象のハードウェアが含まれます。

oemups ユーティリティを使用して UPS を設定できます。UPS エントリを追加するには、以下のコマンドを入力します。

```
oemups -a
```

Vendor Name、**UPS Type**、**IP Address**、**Cabinet ID** パラメータが照会されます。これらのフィールドには最初はデフォルト値(**American Power Conversion**、**APC UPS**、**0.0.0.0, 0**) が表示されます。**IP Address** には、サーバの IP アドレスまたは Web カード搭載の UPS の IP アドレスを入力する必要があります。

次のコマンドを使用して、既存の UPS エントリの一覧を表示できます。

```
oemups -l
```

次のコマンドを使用して、UPS エントリを削除できます。

```
oemups -d <UPS エントリの番号>
```

変更内容は、サーバを再起動しないと反映されないことに注意してください。